Journal of Neurological Disorders

J Neurol Disord
Volume 11:1, 2023

Review Article

Open Access

An Examination of the Role of Big Five Personality Traits, Cognitive Processes and Heuristics on Individuals' Phishing Attack Susceptibility Levels

Chloe Bright, Marika Wziatka and Winfrida Ngaruko*

Department of Computing, Bournemouth University, United Kingdom

Abstract

The current research aims to investigate psychological factors that impact levels of individual susceptibility levels to online phishing attacks. A critical review of existing literature was conducted focusing on relevant factors that affect the level of online risk, including The Big Five Personality traits and cognitive processes such as heuristic based thinking. Also investigated were the impact of urgency cues, online habits, and the Covid-19 pandemic on susceptibility levels. During this literature review, relationships between these factors that are currently mainly unexplored were also established to address gaps in the existing literature and broaden the scope of understanding surrounding this topic.

Keywords: Neurology • Stroke • Treatment • Patients

Introduction

Phishing attacks have a high success rate due to three factors: familiarity, misleading design, and constrained attention [1]. These factors are used to lure victims into engaging with attacks that they believe to be genuine sites. Individuals may then input their private information leading to a compromise of their data and security systems. These cyberattacks play a large role in cyber criminality as "humans continue to be considered as the weakest link in securing systems" [2]. A key part of the effectiveness of phishing attacks is victim's levels susceptibility and a lack of knowledge on how to detect these attacks.

Attackers can be hard to trace due to ease of online anonymity [3] and attacks can be difficult to defend against as they do not present as inherently malicious in nature. When an individual engages with a phishing attack, it may compromise their network's security and allow attackers to infiltrate the network's systems. Attacks may be psychologically harmful to the victim as they made an error in judgement that the communication was authentic.

The main aim of this paper is to ascertain and analyze the influence of the big five personality traits, cognitive processes and the role of heuristics along with other relevant factors on an individual's level of susceptibility to phishing attacks. This is to broaden existing knowledge. The aim will be achieved through a critical review of literature in which:

a) The correlation between the big five personality traits and phishing susceptibility will be explored indicating which traits may contribute to greater vulnerability

b) Cognitive processes and the role of heuristics will be critically analyzed to examine links with phishing susceptibility

c) Relevant factors impacting phishing vulnerability will also be identified and investigated.

Literature Review

Examining correlations between the Big Five Personality traits (openness to experience, conscientiousness, extraversion, agreeableness, neuroticism) and an individual's level of susceptibility to phishing

The big five personality traits categorise a set of characteristics into five behavioural types. Each individual presents a different level of particular traits indicating their main personality type. Following definitions of the big five personality traits, openness to experience is associated with open-minded individuals, who are focused on intellectual pursuits; tend to be independent of judgement with an active imagination [4]. Conscientiousness is attributed to those who have self-discipline, are goal-oriented and tend to follow the rules. Extraversion reflects social individuals who like to be around others, are talkative, energetic, impulsive, assertive and dominant. They tend to experience positive emotions. Agreeableness is associated with individuals who are tolerant, compassionate, modest and cooperative. They value and respect others' opinions and believe people are well-intentioned and honest; therefore they tend to trust others. Neuroticism (mental instability) is attributed to those who tend to experience negative emotions (pessimism, embarrassment and guilt). Those individuals tend to be anxious, nervous, with low esteem and may be hot-tempered.

Personality traits have varying effects on phishing susceptibility levels. Researchers found that certain big five personality traits contribute to higher phishing susceptibility [5-7]. According to H. Parker, et al., individuals who present strong openness, extraversion or agreeableness qualities may be more susceptible to phishing attacks than individuals who display conscientiousness or neurotic personality traits, especially to social media-based phishing. Social media phishing is conducted on social media sites and targeted in the platform's user, usually by utilizing a potential victim's information provided on the site [5].

Personality traits may influence online habits that impact phishing susceptibility levels. H. Parker, et al. found links between personality traits of openness, extraversion and agreeableness [5]. It was indicated that due to these traits, an individual's resulting online habits increase their susceptibility to social media based phishing attacks than neurotic or conscientious individuals. H. Parker, et al. found that high scores

***Address for Correspondence:** Winfrida Ngaruko, Department of Computing, Bournemouth University, United Kingdom, Email ms5531243@bournemouth.ac.uk*

Received: 01-February-2023, Manuscript No. jnd-23-89164; **Editor assigned:** 03-February-2023, PreQC No. P-89164 (PQ); **Reviewed:** 17-February-2023; QC No. Q-89164; **Revised:** 22-February-2023; Manuscript No. R-89164 (R); **Published:** 01-March-2023, **DOI:** 10.4172/2329-6895.11.1.538

in openness, extraversion and agreeableness contribute to increased susceptibility level to social media based phishing attacks as a result of their online habits. Extroverted individuals by virtue of their sociable nature tend to spend more time on social media platforms and regularly engage with other users [5]. Also, individuals scoring high in openness to experience tend to be more curious, creative and are more likely to explore sites and engage in various social media activities. Individuals with higher levels of agreeableness are more likely to confide in people during online interaction, especially on social networking sites. These online habits raise the risk of attack due to increased duration of online activity and sites visited, and the increased number of users interacted with.

In contrast, R. Heartfield, et al., identified the frequency and duration of social media platform use as a protective factor for individuals as usage of a platform increases the individuals' awareness and conversance with the platform, which may help them to detect attacks. Nevertheless, some aspects of habitual use of platforms (such as automatic responses, sharing/liking posts, and unconsciously clicking on links) or email and internet addiction were considered crucial positive predictors of phishing susceptibility [8,9]. Additionally, according to A. Vishwanath habitual use of Facebook in particular was found to be the most significant predictor in a social media-based attack [9]. This may indicate a link between phishing susceptibility and the type of social media platform, and suggest the need for further research to examine the correlation between types of social media sites used and individual's phishing vulnerability levels. Moreover, H. Parker explanation for impacted phishing vulnerability in individuals with agreeableness traits refers to increased trust and therefore links to other aspects of susceptibility research (such as cognitive processing) [5]. However, openness to experience and extraversion levels were correlated only with habitual use of social media platforms increasing online activity and duration.

Personality traits influence perceived risk and trust levels which contribute to phishing vulnerability. J. Cho, et al., explored the phishing susceptibility issue from the perspective of perceived risk and trust, proposing a probability model to predict an individual's vulnerability to phishing. Based on personal traits and levels of perceived trust and risk which impacts decision performance and threat detection accuracy. Researchers argued that individuals make decisions based on levels of perceived risk which are subjective and therefore will be different in a situation depending on the individual's predominant personality traits. As outlined by H. Parker, the successfulness of social media phishing attacks is based on the victim's level of trust and perceived risk, this varies and is dependent on personality traits. Research showed that a higher level of openness contributes to lower level of perceived risk. In contrast, highly neurotic people tend to have higher levels of perceived risk which then decreases levels of phishing susceptibility [10-12]. Additionally, individuals who score high in agreeableness tend to be more trusting, even when uncertain, increasing their susceptibility to phishing attacks. However, F. Enos, et al., argued that individuals with higher agreeableness scores are more able to detect lies which can act as a protective factor against phishing attacks [13]. Perceived trust levels vary depending on the level of perceived risk, which is correlated with levels of optimism, pessimism or realism [6]. For instance, highly neurotic individuals who tend to be pessimistic are more likely to distrust and not engage with phishing attacks, whereas optimistic individuals are more likely to give "credit" when facing uncertainty and thus fall victim to attacks.

The big five personality traits may be linked with cognitive processing and influence phishing susceptibility levels. J. Cho argued that a user's susceptibility to phishing attacks is determined by various cognitive factors such as cognitive biases and tendencies [6]. "Need-for-cognition" is attributed to individuals who tend to utilise rational thinking rather than relying on heuristic thinking during decision making processes, which according J. Cho increases their chances of assessing risks appropriately. Furthermore, J. Cho suggested need-for-cognition was found to be positively linked to openness and conscientiousness levels, and negatively linked with neuroticism [6]. Additionally Y. Ge, et al., argued that email based phishing susceptibility varies for each user depending on the individual's cognitive processing when engaging with an email [7]. Cognitive processing and its correlation with phishing susceptibility will be discussed in more detail in the next section.

Big five personality traits group an individual's' characteristics, abilities and behaviour into five categories, meaning there can be various components that make up a 'personality set'. This may form contradictions in terms of susceptibility to phishing attacks as one 'component' within a particular personality trait may act as a protective factor, whereas other features within the same trait may increase risk. For instance, individuals may score high in openness to experience due to their sociable nature, decreased risk perception and online habits which may lead to greater vulnerability to phishing attacks. A positive correlation between openness levels and phishing susceptibility may be caused by characteristics associated with openness traits, such as sensation seeking and higher curiosity. As outlined by M. Tornblad, curious individuals with a tendency to sensation seek are more susceptible to phishing due to their decreased ability to discriminate between authentic and phishing emails [14]. However, openness to experience is also positively correlated with high learning capability, indicating that these individuals learn quickly and easily acquire knowledge [15,16]. This may act as a protective factor in terms of levels of phishing susceptibility. For instance, due to high learning ability, individuals with more traits of openness were found by M. Pattinson to have a greater ability in detecting phishing emails [17]. Similar contradictions are reflected in individuals with neurotic traits. Anxiety associated with individuals with highly neurotic personality traits may act as a protective factor, as it may deter them from spending long periods online [6,18,19]. However, T. Halevi, et al. argued that neurotic individuals tend to exhibit addictive internet use, and thus may display more vulnerable online behavior [20].

H. Parker et al. proposed a model showing the significance of awareness of certain influences in reducing susceptibility to social media based phishing attacks [5]. The model consists of the following elements: gender, age, online habits; knowledge (Internet experience, phishing education, computer and security knowledge); processing social media content systematically, and the big 5 personality traits. The researchers considered the systematic processing of content as the most significant aspect of the model, as this increases correct identification of deceptive messages due to conscious, in-depth and extensive analysis of the message/information received. Levels of computer and security knowledge were considered to be the second most important protective aspect. Awareness of online habits, gender and age were also important, whilst personality traits were rated as least important as a protective factor. However, personality traits are correlated with online habits and learning abilities influencing model aspects, which may suggest a greater importance and correlation than researchers indicated. Moreover, a relationship between age and personality traits was found that requires further analysis, and in future these particular measures should not be considered separately. For instance, T. Halevi found that females who score high in neuroticism levels are more susceptible to phishing attacks compared to highly neurotic males [20]. The researchers also found that although females are generally more susceptible to phishing than males, females who scored high in conscientiousness traits were found to be less susceptible to phishing than males with high conscientiousness levels [20]. However, I. Alseadoon outlined the positive correlation between high neuroticism and higher levels of phishing susceptibility, regardless of individuals' gender [12].

Recommendations for improvements of the proposed model include considering a greater number of factors and extending analysis of factors to other forms of phishing attacks. Additionally, although researchers included the order of significance for each element regarding phishing susceptibility, it could be helpful to assign particular elements to certain score or point-based values to better explain the interlinking factors impacting susceptibility

levels.

The impact of heuristics and other cognitive processes on phishing attack susceptibility

J. Banks described heuristics as 'mental shortcuts that quickly but non-optimally facilitate decision making' and argued that though they drive much of human behaviour, they can lead to systematic logical errors, known as cognitive biases [21]. Heuristic thinking is developed over time by individuals as shortcuts for more efficient decision-making, especially when heuristic thinking is applied to novel or complex situations. Two ontological-category shortcuts are imperative when individuals evaluate human or technological agents [21]. The Machine Heuristic allows individuals to infer objectivity and systematicity from machine-cues, usually leading to a positive assessment, which then influences an individual's credibility rating on different information types. This is particularly relevant when communicating online, as it could increase susceptibility to cyberattacks if heuristic shortcuts lead individuals to believe a phishing email for example is objectively good, especially when compounded with other typical factors cyber-attackers utilise such as time pressure. The Nature Heuristic attributes goodness when cued by organisms, or attributes badness when cued by non-organisms. Heuristics based judgments can be positive or negative based on past experiences and the situational context. However, these heuristics have not been examined in depth in previous research and require a broader exploration.

When examining the persuasive element of cyberattacks such as phishing attacks in relation to cognitive processes and heuristics, S. Chaiken proposed two cognitive processing models [22]. The first is a systematic model based on an individuals' evaluation of a situation and the relevant arguments found in the persuasive communications. Persuasive cues include correct spelling and grammar, recipient-specific information, and the phishing email/site being professional looking with recognisable logos and endorsements. The second model is heuristics based; individuals subconsciously use low cognitive processing when solving complex problems. Reliance is placed on persuasive cues to enable shortcuts in logical reasoning to save time and cognitive effort, but cyber-attackers manipulate these shortcuts to deceive victims.

X. Luo suggested that time pressure reduces processing effectiveness; a technique cyber-attacker consistently employs [23]. Quality of argument was also examined in phishing attacks and found that individuals are more likely to fall victim if the attackers have high argument quality as they are more likely to detect the threat. These cues can have a significant effect when attackers are persuading potential victims to trust them, as a high level of persuasiveness may mean the individual finds the phishing attack credible without examining it in depth as they would if it was less persuasive, and they were then more suspicious. N. Arachchilage, et al. defined this as 'threat detection' which is the extent to which an individual will be able to successfully pinpoint an attack, however an attack containing more persuasive cues entails less effective threat detection [24]. H. Jones, explored the psychological constructs in individual differences of susceptibility levels and found that the level of ability to distinguish between false and genuine emails was somewhat predicted by levels of sensation seeking and cognitive reflection [25].

R. Chen, et al., investigated the impact of previous phishing attack encounters on an individual's susceptibility levels and suggested that individuals who were previously able to detect attacks would experience higher shock than other users when they then fail to detect an attack [26]. This then raises their susceptibility levels higher than average users. A recent encounter may make an individual realise their susceptibility levels are higher than they thought and drive personal change in their online behaviour. Expectation Confirmation Theory (ECT) R. Chen, et al., suggests that disconfirmation of an individual's beliefs, through expectation and their own perceived performance will influence personal changes [26]. Individuals who have successfully detected cyberattacks in the past may experience high levels of disconfirmation when they fail to detect and then fall victim to an attack. Additionally, individuals who may become desensitised to phishing attacks, such as through repeated exposure to threats, or an emphasis on the danger of cyberattacks in the media may mean individuals start to underestimate online threats as they become overconfident in their attack detection abilities. This is caused by fatigue in the face of high levels of news on cyberattacks and then the disregard of security warnings.

H. Huang, et al. further suggested that user education and knowledge impact susceptibility levels, and P. Kumara guru defended this by stating user education can play a large role in successful threat detection and therefore lower susceptibility levels [27,28]. One of the main limitations of within-situation susceptibility studies that the current research is that it ignores that an individuals' susceptibility to cyberattacks may change over time [26]. This is in contrast to cross-situation susceptibility studies which explore levels of susceptibility as a result of previous experiences across different situations that the victims then learn from. Individuals can use these experiences to improve their cyber-attack susceptibility levels through this knowledge gained when engaging with cyber-attack encounters in the future.

The authors R. Chen, et al. aimed to bridge the literature gap by combining cognitive processes when engaging with a potential cyber-attack and the outcome of this detection, in relation to susceptibility levels [26]. The process of attack detection is the series of actions an individual takes to determine if an online communication is authentic, if their judgement was correct, and if this can affect susceptibility depending on the detection outcome and how difficult detection was. Known complexities that can impact on decision difficulty include task complexity. Heuristic cognitive shortcuts may be utilised to simplify choice processes and solve problems more quickly, especially when encountering preference uncertainty. College students were surveyed, and results found that an individual's susceptibility can be limited by detection process difficulty and failures in detecting recent phishing attack attempts. M. Aburrous, et al. suggested that the outcome of failing to successfully identify an attack has a high psychological cost which may manifest in victims displaying anger, distrust and denial in being able to accept they were victimised [29,30]. Also, it was found past successes in attack detection and being desensitised to attacks through common recurrence was important in regulating any effects of recent encounters.

However, the research could be criticised as their research approach is not generalisable to all populations and can be impacted by individual differences in belief systems [26]. A more holistic approach to understanding susceptibility was recommended for future research since susceptibility level can evolve overtime. By training individuals to successfully detect outcomes in relation to their own prior detection experiences could be advantageous for reducing victim levels. For example, employers could schedule occasional mock phishing tests to avoid employees becoming overconfident or fatigued in their attack detection and are able to evaluate their own susceptibility levels in a safe environment. Limitations of the research include a lack of exploration into an individual's motivations when utilising detection processes, regardless of detection difficulty or outcome. Future studies could examine psychological motivations at different stages of the detection process for a broader understanding. Additionally, future studies could investigate other factors that occur in the detection process that may help regulate detection difficulty or make an individual more likely to detect an attack, and the impact this has on perceived susceptibility levels.

When examining the impact of cognitive processing on phishing scam detection ability, P. Musuva, et al. conducted a university based study in which they sent 4483 test phishing emails to students and staff. Of these emails sent, 241 participants (5.3% of individuals targeted and termed as 'active participants') opened the email and engaged with the phishing stimulus [31]. Results found a total of 98 participants opened the phishing hyperlink (some clicked the link several times). Additionally, the form on

the phishing website was filled in 72 times (6 were repeated entries). This means that 31.12% of active participants who engaged with the phishing link then entered further information into the phishing site. Of these participants, 88% disclosed passwords that would allow an attacker to infiltrate the University's systems.

The authors P. Musuva, et al. stated that even though this was a university based study, it has high ecological validity as the participants were not aware they were being studied [31]. This allowed the researchers to observe how the participants would typically engage with phishing attacks as they did not modify their behaviour, meaning the research design could be reused in other participant populations. Additionally, the research is highly relevant as research has shown university students are specifically targeted in many cyberattacks as they are susceptible to falling victim to attacks [32]. Thus, universities spend a significant amount on resources to protect students from cyberattacks [33].

Spear phishing attacks are variant phishing attacks that are targeted at specific individuals such as government figures or individuals with insider knowledge of industrial control systems. Spear phishing attacks can be utilised in espionage and terrorism attacks which makes it a particularly dangerous cyber-security threat. The effectiveness of cyber-security training has been demonstrated by L. Ponemon, a 64% decrease in clicking spear phishing links was reported in a survey by 377 U.S based IT practitioners after implementation of training [34]. Additionally D. Caputo, et al. stated that the number of individuals engaging with spear-phishing links decreased by 63% after cyber-security training was implemented with a focus on detecting simulated spear phishing emails [35]. However, this research could be criticised as the research sample consisted of 1,395 participants from an organisation based in Washington DC, meaning it is less generalisable to the public and novice online users. X. Luo, et al. conducted a field study that examined a spear phishing attack which targeted 105 people at an American university, basing their research on the systematic model of heuristic processing [23]. Results found that whilst 64% of users targeted did not engage with the attack, 36% of targeted users engaged with the phishing link, and a further 15% of these individuals who engaged with the link then submitted their login credentials on the phishing site, which would have compromised the university's systems in a genuine attack.

Y. Kwak, et al. based their research on A. Bandura Social Cognitive Theory to explore why individuals do not report cyberattacks, with a focus on spear phishing attacks, even though they are encouraged to do so in cyber awareness training [36,37]. A focus on three factors of the SCT model were examined. According to the theory these factors motivate human actions: influence of perceived self-efficacy of susceptibility to attacks, individuals' cyber safety behaviours, and expected negative outcomes from reporting attacks. This was investigated in accordance with how these factors influence individuals' likelihood to report attacks. In the SCT framework, the stage of forethought allows individuals to process outcome negative or positive expectations [38], whilst individuals' metacognitive processes allow constructs of self-efficacy. This describes how confident an individual is at performing behaviours [39]. J. Wang, et al. stated that individuals with high self-efficacy levels in attack detection showed stronger ability when utilising detection behaviours, such as analysing persuasive cues in a spear phishing email to evaluate credibility [40]. Self-Monitoring in SCT is the ability to observe and calibrate intended behaviours, and then perform behaviours based on the necessary response required.

It was found that higher self-efficacy levels and acts of self-monitoring encouraged the use of security software and encouraged displays of security conscious behaviours that further safeguard individuals. These include not sharing sensitive information online and using strong passwords [41]. However, a criticism of previous self-efficacy and self-monitoring studies are that the effectiveness of these behaviours are limited by the failure to comply with cyber-security recommendations made during user awareness training. D. Caputo Users may also relapse into habitual patterns of online behaviour and email use which may re-increase susceptibility after training [35,42].

Y. Kwak, et al. incorporated Cyber Risk Beliefs (CRBs) combined with SCT framework in relation to cyber-attack susceptibility [36]. CRBs are defined as individuals' perceptions about inherent risks associated with online behaviour. High CRBs are important in lowering individuals' susceptibility to spear phishing attacks as it encourages utilising cognitive resources to examine potential attacks. CRBs motivate systematic processing which raises suspicion when engaging with online communications. In contrast, lower CRB levels increase susceptibility to spear-phishing attacks as they encourage a reliance on heuristic based thinking. E. Williams, et al. suggested that CRBs of risk perception, combined with systematic information processing that arouses suspicion indeed have a negative impact on individual's susceptibility levels to cybe-rattacks [43]. When CRBs and SCT elements are combined the CRBs impact the amount of cognitive effort individuals exert, but also impact reporting likelihood [33]. Results garnered from the current research survey data of 386 participants showed that the high levels of self-efficacy and cyber-security self-monitoring behaviours and awareness increased the intention to report spear phishing attacks, which then allows earlier detection by IT departments before the attack spreads further [36]. Additionally, expected negative outcomes and an individual's own CBRs positively influence intention to report spear phishing emails and encourage optimal online safety behaviours. CRBs directly influenced the three SCT factors and indirectly impacted the likelihood of reporting attacks, adding to existing literature of cyber-security linked with cognitive theories.

The literature has important implications for cyber-security practices, as it suggests that individuals with higher self-efficacy levels are more concerned with the expected negative outcomes that may result from reporting spear-phishing attacks. Future suggestions for cyber-security attack awareness include improving communication between individuals reporting attacks and the system collecting reports of attacks to encourage reporting levels. Furthermore, improvement of individuals' self-monitoring could enhance cognitive processes, leading to improved attack detection accuracy and a reduction in online habituation behaviour. In contrast, criticisms of the current research include the use of a student sample, which while it allows for internal validity and convenience lacks ecological validity as it is not representative to other populations. Researchers may also not be able to apply university based sample results to professional organisational structures and existing security practices, plus social norms and workplace cultural factors that could influence reporting rates.

Another criticism is that whilst measures for CRBs and cyber-security self-efficacy behaviours were established in previous research, the authors had to create their own measures for expected negative outcomes of reporting attacks, cyber-security self-monitoring behaviours, and likelihood of reporting attacks. While the measures were statistically proven as reliable, future research is required to broaden the scope of understanding. Additionally, recommendations include testing the validity of the model in other cyber-attack forms such as social media scams and ransom ware. The research population should also be widened to company organisations, different levels of online experience, and wider age ranges. The number of participants that fell for the false spear-phishing attacks was also not reported [36], as well as how negative outcomes can affect an individual emotionally and impact susceptibility awareness could also be further explored.

Other factors that may influence an individual's phishing susceptibility

Gender: Previous gender-phishing susceptibility research yielded inconsistent findings though most found that females were more prone to fall for phishing emails. In a 2011 phishing study of university students, teachers and staff, men were better at identifying phishing emails than

females [44]. Similarly, in a phishing experiment with 487 18–24 year old students, women were more likely to fall for phishing than males [45]. S. Sheng, et al. also discovered that women were more sensitive to phishing in a survey and role-playing research with 1,001 Amazon.com Mechanical Turk participants although females in this study had less technical expertise [32]. Although this implies that females are more susceptible to fall victim to phishing attacks, it should be noted that phishing can affect both men and women although other variables such as technical knowledge may be involved.

Age: In the online survey and role-playing research, 18–25 year olds were more inclined to click on phishing emails. This is because younger people may participate in more dangerous online behaviours [32]. In a 21 day phishing campaign, found that older groups, especially older women were more vulnerable to phishing [46]. This may be because the elder generation may struggle to keep up with technology's continual progress. D. Sarno, et al. examined phishing susceptibility in young and older email users [47]. They found that younger people classified emails as authentic, whereas older adults classified them as phishing. As with gender focused studies, age and phishing susceptibility research have also shown contradictory findings owing to methodological discrepancies. Age alone may not strongly indicate phishing susceptibility although it may correspond with other more basic issues.

Technical experience: A person's vulnerability to social engineering and phishing may be affected by their level of technical competence, which can include both past usage of technology and training in its use. Training has proven one of the most effective defences against these types of assaults [48]. Through experience, one may develop a heightened awareness and attention for suspicious emails. If cyber-security training and awareness campaigns are to lessen phishing risk, they should emphasise the need of developing safe cyber-security habits. As a result, a person's level of technical expertise, familiarity with information technology security policies and practices, and habits about the performance of cyber-security protection procedures while at work are crucial indications of phishing vulnerability.

Urgency cues: Users are forced into deadlines because of phishing emails. According to the psychological reactance hypothesis, people prefer limited and competing resources [49]. Threat makes use of the scarcity principle by providing incentives for quick action and penalties for delayed response [49]. Consumers are frightened into responding quickly by the threat of incurring penalties, which might result in a reduction in their credit score or the suspension of their account. Users were coerced into complying with legal phrases such as "kindly abide" and "hereby demanded" [49]. Email recipients are expected to follow the action that is most straightforward [50]. It is possible that ideas proposed through email will factor into this choice. Therefore, the mental pressure that is generated by a large volume of emails makes it more difficult to detect phishing attacks. Therefore, indications in email communications that increase feelings of urgency may increase susceptibility to phishing.

Trust cues: Phishing emails build trust [39]. Most phishing emails look like legitimate emails from credible sources and this makes it easier to gain trust from victims because of their familiarity.

R. Naidoo states that phishing emails should meet three trust-building requirements. Familiarity is the first trust criteria such as an individual recognising an email as being from their bank and therefore trusting the content [49,50]. Secondly, as individuals have trusted prior emails from their bank, the phishing email must be similar to the style of these authentic prior emails. Since banks have a large client base and are known for the identity of their brand, cyber-attackers may choose to join banks as members, allowing them access to prior email correspondences and brand information. They will then utilise these sources to replicate high quality phishing attack content. Thirdly, the attack design should look polished and professional to encourage trust from the receiver. Trust affects factors including cognition processes, emotions, and compliance levels. Since an individual is likely to engage with their bank on a regular basis, users tend to display obedience to the bank given uneven power levels in the relationship between bank and individual. Users develop trust overtime in their bank and begin to identify strongly with the bank, so they place a reliance on patterns when making future judgments. Cyber attackers utilise this decision-making methodology to their advantage, targeting users as they trust their previous experiences with banking correspondences.

Knowledge: Knowledge may impact vulnerability to phishing scams. Knowledge underpins phishing detection. Users cannot identify authentic from inauthentic phishing emails without prior knowledge [51]. S. Sheng, et al. revealed that trained participants are less vulnerable to phishing [32]. Knowledge of phishing improves detection. Knowing other domains might also help consumer's spot fraudulent emails. For example, bank employees' familiarity with bank emails means they are more likely to spot strange indications in phishing emails related to banking. Studies show that those who are more tech-savvy can detect and engage with phishing emails more effectively [17]. Explicit and implicit knowledge exist. The distinction between explicit and implicit information is that explicit knowledge may be validated as true or untrue, but implicit knowledge can be gained fast from personal experience or through another person [52]. Learning and direct training provide explicit information, while experiences of phishing attacks boost implicit knowledge. A. Baillon, et al. tested direct and embedded teaching in a simulated phishing campaign. Both forms of training can enhance users' phishing detection skills, but embedded training is more successful because falling for a phishing attack can boost their awareness when engaging with future phishing attacks [53]. Studies show that knowledge directly affects phishing vulnerability [51]. The more someone has knowledge on how to distinguish a real email from a fake email then the less susceptible this person is to fall for the phishing tactics used by threat actors. Knowledge affects how users react to phishing emails and their in-the moment state.

Perception and beliefs: Our perceptions of risks, efficacy, and confidence affect phishing detection performance. A situation's perceived threat is subjective. Perceived threat includes severity and susceptibility. Perceived severity is one's belief about the threat's size and impact. C. Canfield, et al. study examining email management indicated that more negative repercussions result in detecting more phishing emails [54]. Thus, while this could help reduce phishing attack susceptibility, it will also increase false positive detection outcomes. J. Wang, et al. found that more perceived threats are positively associated with levels of phishing attack anxiety which may cause higher risk online behavior [40]. Perceived susceptibility is the individual's self-perceived likelihood of them falling victim to a phishing attack. J. Wang, et al. observed that a higher perceived susceptibility to being phished can impair detection performance [40]. The response efficacy describes the individual's beliefs about the effectiveness of the proposed response in dealing with the threat, and the perceived self-efficacy describes their ideas about their capacity to carry out the response [51]. The need for protection against cyberattacks motivates response efficacy. Higher perceived self-efficacy levels motivate phishing victims to avoid engaging with potential phishing emails as higher self-efficacy levels result in higher confidence levels when engaging with potential attacks. C. Canfield, et al. noted that increased confidence is associated with a higher likelihood of deeming an email as legitimate [54]. Overconfidence can make them ignore potential phishing elements of emails, putting them at risk [40], and other beliefs may make users careless about phishing attacks, meaning they are more likely to fall victim to attacks.

Mental illness: Phishing vulnerability may be increased in those with mental disorders. Individuals with psychological vulnerabilities, such as those suffering from severe mental illness or elderly people, are often targets for several types of financial fraud [55]. People who are emotionally unstable or impulsive are more likely to lose money in online fraud attacks [56]. When mentally ill people are experiencing psychotic episodes, or cognitive and memory impairments, they may make online judgments that put them at

risk, such as engaging with phishing emails.

Online habits: Higher social media usage increases vulnerability to social media phishing attempts [9]. Active social media users are more vulnerable to social engineering attempts [9]. Online behaviour also affects how people react to social engineering techniques on social media sites [57]. Negative online behaviours may increase vulnerability to attacks because individuals may instinctively click on links and reply to messages without utilising adequate cognitive resources, or paying attention to their online behaviour [39]. For instance, frequent Facebook users are more likely to fall victim to accounts with fake identities, and then provide phishers sensitive personal information [9]. Furthermore, online habituation behaviours may result in people utilising social media in ritualised ways that require less cognitive attention, increasing susceptibility to phishing attacks [57]. This increases the likelihood that individuals click on dangerous links in messages or accept friend requests from fraudulent profiles without considering the potential repercussions [9]. Social media users may engage with dubious content by clicking on phishing links, sharing and liking posts, and skimming through posts [58]. Therefore, online habits may increase self-efficacy in risk perception and make individuals over-confident, making users more vulnerable to social media based phishing attacks.

Emotions: According to N. LeFranc, phishers focus on the emotions of their victims [59]. Cyber-attackers take advantage of users' lack of knowledge, gullibility levels, the need to be liked, and their desire to help others. When individuals are experiencing intense feelings, it activates their subconscious processes, which in turn makes them more inclined to share personal information. Phishing attackers take advantage of the fact that the subconscious mind does not operate in a rational or analytical manner [58]. When workers receive a phishing email that is from their employer, their emotional connection to the company may cause them to feel anxious, clouding their judgement and making them more susceptible to phishing attacks. N. LeFranc claimed that emotions influence workers' responses to phishing emails [59]. N. LeFranc also argued that an employees' emotional attachment to their organisation, normative commitments and a strong sense of urgency can evoke emotional reactions when they receive a phishing email, which can increase their phishing susceptibility [59].

COVID-19: According to a study conducted by Tessian, employees receive an average of 14 phishing emails per year [60]. Particularly affected were retail employees who received an average of 49 phishing emails per year. From the months of May to August in 2021, email-based assaults increased by 7.3%. Phishing based emails accounted for most of these attacks, according to ESET's 2021 study [61]. IRONSCALES' most recent study indicates that since March 2020, email phishing attacks have increased in 81% of enterprises worldwide [62]. The study also found that whilst phishing attacks continually grow in prevalence and sophistication, only 1 in 5 enterprises provide their staff with phishing awareness training annually. Additionally, 25% of all data breaches involve phishing, and 85% of data breaches have a human component, according to Verizon's 2021 Data Breach Investigation Report [62].

Throughout and after the COVID-19 pandemic, levels of phishing attacks have escalated, leading to companies and people being compromised. A scoping study Y. He, et al. found significant factors that increase susceptibility to phishing and other cyber-attacks [63]. Firstly, the reduced mobility due to countries' lockdowns and restrictions to travel necessitated more working from home and distant labour. Secondly, employees with no experience or training were unexpectedly moved to remote work environments. Third, personal communications require experience with digital communication technologies. This then exposed service employees and users to various cyber-attack threats [63].

The three preceding vulnerabilities influence every area of society. Due to unique circumstances during the pandemic and their crucial role, healthcare and government services were more susceptible to cyberattacks. These industries had more vulnerability because of poor digital literacy [64]. Attacks on these targets became increasingly frequent and more lucrative. Phishing attempts often lured victims into revealing sensitive information by various means like attackers offering highly sought after personal protective equipment (PPE) [65].

The impact of the pandemic caused severe stress, worry, and uncertainty that made people more susceptible to phishing attacks [66]. The research shows those individuals' fear of COVID-19 encouraged users to frequently engage with emails from health organisations like the WHO (World Health Organization) to read the newest health and vaccination advice [67]. Research found that fraudsters generated ad-hoc phishing communications that mimicked government announcements to increase their credibility and success [66]. The time between an official statement and attackers utilising the communication to their own advantage was often quite brief, such as two days, which helped increase victimhood and diminish a user's ability to detect attacks.

Cybercriminals also use COVID-19-related anxiety to commit cyber fraud. According to K. Ma, 30% of cyber fraud occurrences include hackers approaching victims with relief, 22% with fear, and 22% with hope. Cyber fraud also utilises delight (15%), threat (6%), and compassion (5%) [68]. Cybercriminals may spread misinformation about cures/treatments, or government relief funds to utilise feelings of relief or hope to attract targeted victims. To facilitate feelings of fear or threat, they may circulate COVID-19-related pressures, such as false alerts about local outbreaks, or use intimidating virus-related images to make victims feel vulnerable and concerned [69]. Cybercriminals may also appeal to victims' emotions to encourage them to buy entertainment services or believe they are donating to the needy [68]. Research shows that cybercriminals use positive emotional pleas to trick victims into donating money throughout the pandemic.

COVID-19 anxiety may make one more susceptible to regular and COVID-19 based phishing attacks [67]. When impacted by fear regarding the pandemic, a person may be more likely to engage with a phishing link or open attachments without thinking. Thus, highly anxious users may not be able to properly utilise phishing detection techniques when previously in a low anxiety state they would have been able to more effectively. The pandemic has also affected mental health related to online behaviour. COVID-19 societal stigma may affect behaviour and mood. Considering the psychological backdrop, COVID-19 based cyberattacks may use victims' levels of stress, anxiety, and other emotional weaknesses to their advantage [69].

Discussion

Individuals scoring high in openness, extraversion, and agreeableness tend to be more susceptible than those who score high in neuroticism or conscientiousness. Investigating different components within personality traits could help achieve a more in depth relationship with susceptibility levels to phishing attacks, helping to indicate which components of an individual's personality most affect levels of susceptibility. This is especially important as an individual may not display one predominant personality trait but present similar scores in different traits, where their correlation to phishing susceptibility is inverse. Moreover, an indication of when the value should be considered high enough to have a correlation with phishing susceptibility would be useful for vulnerability assessment. Additionally, personality traits influence online habitual behaviour and are linked with other factors (such as gender or age) that play a role in levels of phishing susceptibility. Identifying regularly occurring characteristics of victims could be beneficial in increasing the scope of understanding regarding the relationship between personality types and susceptibility to phishing attacks.

Conclusion

Heuristics were found to be non-optimal cognition shortcuts that are utilised when engaging with complex problems such as attempting to detect a phishing attack. Heuristics have been found to increase the level of phishing attack susceptibility as they lead to cognitive biases in which an individual will automatically deem something as inherently bad or good. This finding was also interlinked with social engineering techniques commonly used by attackers, such as persuasive cues and time pressure, which can decrease the success of threat detection. Additionally, it was found that repeated exposure to phishing attacks can lead to mental fatigue and thus non-optimal cyber-security practices and riskier online behaviour, making an individual increasingly more susceptible to attacks. Frequent cyber-security training is recommended to encourage users to report attacks and minimise individuals reverting back to risky habitual online behaviour. Overall, understanding and incorporating cognitive processes into cyber-security training would be beneficial in the future to decrease levels of susceptibility and thus decrease the level of successful attacks over time.

To considerably raise the likelihood of a person falling victim to phishing attempts, demographics (age and gender) must be paired with other characteristics such as technological expertise and technical understanding. The kind of wording used in a phishing email might activate trust or urgency cues in the receiver, which, if acted upon, can increase their likelihood of falling victim to phishing. It was also shown that an individual's self-perception significantly increased the likelihood of being phished. Individuals who overestimated their ability to detect phishing scams were more likely to fall victim to them than to identify them. Frequent social media users exhibited dangerous online habits, making them vulnerable to phishing attacks. As the mind would be in a vulnerable state and appropriate decision making would be difficult, mental illness might potentially make an individual more susceptible to phishing assaults.

COVID-19 brought up several adverse consequences, such as despair and anxiety, which threat actors used in their phishing schemes. Due to COVID-19 fear, communications containing any information regarding COVID-19, such as vaccination emails, were considered as authentic even when they were not, resulting in more individuals falling prey to phishing schemes.

Phishing susceptibility was found to correlate with psychological influences such as the big five personality traits, heuristics and cognitive processes. These elements may make certain individuals more or less susceptible, and the current research indicates the need to explore phishing issues from a psychological perspective to develop more effective solutions. Additionally, demographic and other related factors along with current societal situations (such as COVID-19) contribute and influence an individual's level of susceptibility to phishing attacks.

The complexity of this paper and the novelty of exploring these factors separately and together help to broaden the scope of knowledge on phishing susceptibility through analysis of literature gathered from different viewpoints and contributors. The examination of cyber-security factors and explanations for individuals' susceptibility levels from commonly overlooked psychological perspectives could help cyber-security expert's work with cyber psychologists to develop cyber-security training programs in the future.

In future research, the current analysis could be extended further through the exploration of links established between elements investigated and how they interact with each other. This could provide a more in depth picture of relevant influences and lead to detailed identification of protective and risk factors and allow investigation of which aspects of an element have a greater importance and to what extent they influence each other. Further analysis could explore these correlations and perhaps extend to different types of phishing attacks, such as ransom ware, as factors affecting susceptibility levels may vary depending on the cyber-attack.

Conflicts of Interest

It is declared that there is no conflict of interest.

References

1. McNealy, J. "Platforms as Phishing Farms: Deceptive Social Engineering at Scale." *New Med Societ* 24(2022): 1677-1694.
2. Sharma, T and Bashir M. "An Analysis of Phishing Emails and How the Human Vulnerabilities are Exploited." *Adv Hum Fact Cybersec* 1219(2020): 49-55.
3. Vayansky, I and Kumar S. "Phishing - Challenges and Solutions." *Comp Fraud Secur* 2018(2018): 15-20.
4. Frauenstein, E and Flowerday S. "Susceptibility to Phishing on Social Network Sites: A Personality Information Processing Model." *Comp Secur* 94(2020): 1-18.
5. Parker, H and Flowerday S. "Contributing Factors to Increased Susceptibility to Social Media Phishing Attacks." *Sajim* 22(2020): 1-10.
6. Cho, J, Cam H and Oltramari A. "Effect of Personality Traits on Trust and Risk to Phishing Vulnerability: Modeling and Analysis." *IEEE Conferences* 2016.
7. Ge, Y, Lu L, Cui X and Z. Chen, et al. "How Personal Characteristics Impact Phishing Susceptibility: The Mediating Role of Mail Processing." *Appl Ergonom* 97(2021): 103526.
8. Heartfield, R, Loukas G and Gan D. "You are probably not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks." *IEEE Access* 2016.
9. Vishwanath, A. "Habitual Facebook Use and its Impact on Getting Deceived on Social Media." *J CompMedia Comm* 20(2015): 83-98.
10. Tupes, E and Christal R. "Recurrent Personality Factors based on Trait Ratings." *J Pers* 60(1192): 225-251.
11. Chauvin, B, Hermand D and Mullet E. "Risk Perception and Personality Facets." *Risk Anal* 27(2007): 171-185.
12. Alseadoon, I. "The Impact of Users' Characteristics on Their Ability to Detect Phishing Emails." *Adv Comp Comm Engg Technol* 315(2014): 949-962.
13. Enos, F, Benus S, Cautin R and Graciarena M, et al. "Personality Factors in Human Deception Detection: Comparing Human to Machine Performance." *The Ninth International Conference on Spoken Language Processing*, 2006.
14. Tornblad, M, Jones K, Namin A and Choi J. "Characteristics that Predict Phishing Susceptibility: A Review." *Proc Hum Fact Ergons Soc Ann Meet* 65(2021): 25-34.
15. Chamorro-Premuzic, T and Furnham A. "Mainly Openness: The Relationship between the Big Five Personality Traits and Learning Approaches." *Learn Ind Diff* 19(2009): 524-529.
16. Barrick, M and Mount M. "The Big Five Personality Dimensions and Job Performance: A Meta-Analysis." *Person Psychol* 44(1991): 1-26.
17. Pattinson, M, Jerram C, Parsons K and McCormac A, et al. "Why do Some People Manage Phishing E-Mails Better than Others?." *Info Manag Comp Secur* 20(2012): 18-28.
18. Aguilar, LA and Solanas A. "Human Susceptibility to Phishing Attacks Based on Personality Traits: The Role of Neuroticism" *IEEE Annual International Computer Software and Applications Conference*, 2021.

19. Weirich, D and Sasse M. "Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World." *in ACM Proceedings of 10th Workshop on New Security Paradigms*, 2001.

20. Halevi, T, Lewis J and Memon N. "A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits." *Proceedings of the 22nd International Conference on World Wide Web*, 2013.

21. Banks, J, Edwards A and Westerman A. "The Space Between: Nature and Machine Heuristics in Evaluations of Organisms, Cyborgs and Robots." *Cyberpsychol Behav Soc Netw* 24(2021): 324-331.

22. Chaiken, S. "Heuristic Versus Systematic Information Processing and the Use of Source Versus Message Cues in Persuasion." *J Personal Soc Psychol* 39(1980): 752.

23. Luo, X, Zhang W, Burd S and Seazzu A. "Investigating Phishing Victimization with the Heuristic–Systematic Model: A Theoretical Framework and an Exploration." *Comp Secur* 38(2013): 28-38.

24. Arachchilage, N and Love S. "A Game Design Framework for Avoiding Phishing Attacks." *Comp Hum Behav* 29(2013): 706-714.

25. Jones, H, Towse J, Race N and Harrison T. "Email Fraud: The Search for Psychological Predictions of Susceptibility." *PLoS One* 14(2019): e0209684.

26. Chen, R, Gaia J and Rao H. "An Examination of the Effect of Recent Phishing Encounters on Phishing Susceptibility." *Dec Supp Syst* 133(2020): 113287.

27. Huang, H, Tan J and Liu L. "Countermeasure Techniques for Deceptive Phishing Attack." *International Conference on New Trends in Information and Service Science*, 2009.

28. Kumaraguru, P, Sheng S, Acquisti A and Cranor L, et al. "Teaching Johnny not to Fall for Phish," *ACM Transac Int Technol* 10(2010): 1-31.

29. Aburrous, M, Hossain M, Dahal K and Thabtah F. "Experimental Case Studies for Investigating E- Banking Phishing Techniques and Attack Strategies." *Cognit Computat* 2(2010): 242-253.

30. Finn, P and Jakobsson M. "Designing Ethical Phishing Experiments." *IEEE Technol Soc Magazine* 26(2007): 46-58.

31. Musuva, P, Getao K and Chepken C. "A New Approach to Modeling the Effects of Cognitive Processing and Threat Detection on Phishing Susceptibility." *Comp Hum Behav* 94(2019): 154-175.

32. Sheng, S, Holbrook M, Kumaraguru P and Cranor L, et al. "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions." *Proceedings of the SIGCHI conference on human factors in computing systems*, 2010.

33. Vishwanath, A, Harrison B and Ng Y. "Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility." *Commun Res* 45(2018): 1146-1166.

34. Ponemon, L. "The Cost of Phishing and Value of Employee Training." *Ponemon Institute*, 2015.

35. Caputo, D, Pfleeger S, Freeman J and Johnson M. "Going Spear Phishing: Exploring Embedded Training and Awareness." *IEEE Secu Privac* 12(2014): 28-38.

36. Kwak, Y, Lee S, Damiano A and Vishwanath A. "Why Do Users not Report Spear Phishing Emails?" *Telemat Inform* 48(2020): 101-343.

37. Bandura, A. "Social Foundations of Thought and Action." 1986.

38. Rose, RL, Lin C and Eastin M. "Unregulated Internet Usage: Addiction, Habit, or Deficient Self- Regulation?," *Media psychol* 5(2003): 225-253.

39. Vishwanath, A, Herath T, Chen R and Wang J, et al. "Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model," *Decis Supp Syst* 51(2011): 576-586.

40. Wang, J, Li Y and Rao H. "Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences." *Infor Syst Res* 28(2017): 378-396.

41. Rhee, H, Kim C and Ryu Y. "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior" *Comput secur* 28(2009): 816-826.

42. Vishwanath, A, "Examining the Distinct Antecedents Of E-Mail Habits and its Influence on the Outcomes of a Phishing Attack" *J Comp Mediat Comm* 20(2015): 570-584.

43. Williams, E, Beardmore A and Joinson A. "Individual Differences in Susceptibility to Online Influence: A Theoretical Review" *Comput Hum Behav* 72(2017): 412-421.

44. Blythe, M, Petrie H and Clark J. "F for Fake: Four Studies on How We Fall for Phish." *CHI Conference on Human Factors in Computing systems, Vancouver*, 2011.

45. Jagatic, T, Johnson N, Jakobsson M and Menczer F. "Social Phishing." *Comm ACM* 50(2007): 94-100.

46. Lin, T, Capecci D, Ellis D and Rocha H, et al. " Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content." *ACM Trans Comput Hum Interact* 26(2019): 1-28.

47. Sarno, D, Lewis J, Bohil C and Neider M. "Which phish is on the Hook? Phishing Vulnerability for Older Versus Younger Adults." *Hum Factors* 62(2020): 704-717.

48. Parrish, J, Bailey J and Courtney J. "A personality Based Model for Determining Susceptibility to Phishing Attacks." *Southwest Decision Sciences Institute Conference* (SWDSI '09), 2009.

49. Naidoo, R. "Analysing Urgency and Trust Cues Exploited in Phishing Scam Designs." *in 10th International Conference on cyber warfare and security*, 2015.

50. Ayaburi, E and Baidoo AF, "Understanding Phishing Susceptiibility: An integrated Model Of Cue-Utilization and Habits." *40th International Conference on Information Systems* (ICIS) 2019, 2019.

51. Zhuo, S, Biddle R, Koh R, Lottridge D and Russello G. "SoK: Human-centered Phishing Susceptibility." *arXiv* 2022.

52. Clime, E. "The Three Types of Knowledge: Explicit, Implicit and Tacit."

53. Baillon, A, De Bruin J, Emirmahmutoglu A and Van DBE, et al. "Informing, Simulating Experience, or Both: A Field Experiment on Phishing Risks." *PLoS one* 12(2019): e0224216.

54. Canfield, C, Fischhoff B and Davis A. "Better Beware: Compairing Metacognition for Phishing and Legitimate Emails." *Metacog Learn* 14(2019): 343-362.

55. Lichtenberg, P, Sugarman M, Paulson D and Ficker L, et al. "Psychological and Functional Vulnerability Predicts Fraud Cases in Older Adults. Results of a Longitudinal Study." *Clin Gerontol* 39(2016): 48-63.

56. Whitty, M. "Is there a Scam for everyone? Psychologically Profiling Cyberscam Victims" *Europ J Cril Pol Res* 26(2020): 399-409.

57. Frauenstein, E and Flowerday S. "Social Network Phishing: Becoming Habituated to Clicks and Ignorant to Threats?" *15th International Conference on Information Security*, 2016.

58. Chaudhary, S. "The Use of Usable Security and Security Education to Fight Phishing Attacks" *University of Tampere*, 2016.

59. LeFranc, N and Savoli A. "Factors Influencing employees' Susceptibility to Phishing Emails: The Role of Emotions." *13th Mediterrenean Conference on Information Systems (MCIS), Naples*, 2019.

60. Tessian "What is Business Email Compromise (BEC)? How does it work?," *Tessian*, 2021.

61. Rosenthal, M. "Must Know Phishing Statistics: Updated 2022." *Tessian*, 2022.

62. Jones, C. "50 Phishing Stats you should Know in 2022." *Expert Insights*, 2022.

63. He, Y, Aliyu A, Evans M and Luo C. "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review." *J Med Internet Res* 23(2021): e21747.

64. Sardi, A, Rizzi A, Sorano E and Guerrieri A. "Cyber Risk in Health facilities: A Systematic Literature Review." *Sustainability* 12(2020): 7002.

65. Al-Qahtani, A and Cresci S "The COVID-19 Scamdemic: A Survey of Phishing Attacks and their Countermeasures during COVID-19." *IET Inf Secur* 16(2022): 324-345.

66. Lallie H, Shepherd L, Nurse J and A. Erola, et al, "Cyber security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic." *Comp Secur* 105(2021): 102248.

67. Abroshan, H, Devos J, Poels G and Laermans E. "COVID-19 and Phishing: Effects of Human Emotions, Behaviour and Demographics on the Success of Phishing Attempts during the Pandemic." *IEEE* 9(2021): 121916-121929, 2021.

68. Naidoo, R. "A Multi-Level Influence Model of COVID-19 Themed Cybercrime." *Europ J Inform Syst* . 29(2020): 306-321.

69. Ma K and McKinnon T. "COVID-19 and Cyber Fraud: Emerging Threats during the Pandemic." *J Financ Crime* 29(2021): 433- 446.

How to cite this article: Bright, Chloe, Marika Wziatka and Winfrida Ngaruko. "An Examination of the Role of Big Five Personality Traits, Cognitive Processes and Heuristics on Individuals' Phishing Attack Susceptibility Levels." *J Neurol Disord*. 11 (2023):538.